HSPD-12/FIPS-201
A Short History & Primers for PIV-I & PIV-II Deployment and Integration

Presented by

John Foxx Bissell

Director of Strategic Accounts

Lenel Systems International

jbis@lenel.com

Agenda

- Agenda
  - Definitions of Terms Used
  - HSPD-12 Background
  - FIPS 201
    - History
    - Current Status (PIV I)
      - PIV I Implementation
        - Graphic Overview
        - Implementation Solutions
        - PIV-I ID Components
        - PIV-I Workflow
    - End Game (PIV II)
      - PIV II Implementation
        - Graphic Overviews
        - Key Issues to Convergence 1
        - Key Issues to Convergence 2
        - Migrating from PIV-I to PIV-II
    - Conclusion

Definitions

- PIV – Personal Identity Verification
- IDMS – Identity Management System
- Applicant – Individual to whom a PIV credential is to be issued.
- Employer/Sponsor – Individual who substantiates the relationship to the Applicant and provides sponsorship to Applicant.
- Enrollment Official – Individual who initiates the chain of trust for identity proofing and delivers enrollment package to the IDMS.
- Approval Authority – Entity that establishes organization chain of command within the IDMS for PIV approval.
- Issuing Authority – Entity that issues the PIV credential to the Applicant after all identity proofing, background checks, and related approvals have been completed.
- PACS – Physical Access Control System
- HSPD-12 – Homeland Security Presidential Directive 12
- FIPS-201 – Federal Information Processing Standard 201

- From the President's FY 98 Budget: "The Administration wants to adopt 'smart card' technology so that, ultimately, every [Federal] employee will be able to use one card for a wide range of purposes, including travel, small purchases, and building access."

- From Deputy Secretary of Defense on 11/10/99: "The initial implementation of smart card technology shall be effected as a Department-wide common access card (CAC). The CAC shall be the standard ID card for active duty military personnel, DoD civilian employees and eligible contractor personnel. It also will be the principal card used to enable physical access to buildings and controlled spaces and will be used to gain access to the Department's computer networks and systems."

- From HSPD-12 on 8/27/04: "As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard [FIPS 201], the heads of executive departments and agencies shall, to the maximum extent practicable, require the **use of identification** by Federal employees and contractors that meets the Standard in gaining **physical access to Federally controlled facilities** and **logical access to Federally controlled information systems**."

FIPS 201 Companion Documents

- NIST Special Publication 800-73 (SP 800-73) – April 2005Interfaces for Personal Identity Verification
- NIST Special Publication 800-76 (SP 800-76) – Draft Biometric Data Specification for Personal Identity Verification
- NIST Special Publication 800-78 (SP 800-78) – February 2005 Recommendations for Cryptographic Algorithms and Keys Sizes
- A companion document that is essential for implementing a PIV PACS is the - “Technical Implementation Guidance (TIG): Smart Card Enabled Physical Access Control Systems – Version 2.2” (PACS 2.2). July 30, 2004
- This document was published by the Physical Access Interagency Interoperability Working Group (PAIIWG) of the Smart Card Interagency Advisory Board (IAB).

Current Status

- PIV-I satisfies the control objectives and meets the security requirements of HSPD 12.

- PIV-II meets the technical interoperability requirements of HSPD 12.
  - PIV-II specifies implementation and use of identity credentials on integrated circuit cards for use in a Federal personal identity verification system

(extract from page V FIPS 201)

PIV I Identity Verification and Issuance

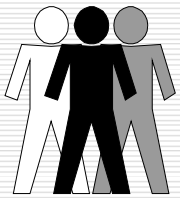
1

2

Employer Sponsorship

3

Approval Authority



Employee Application

Employee Enrolls

5

Identity Management System (IDMS)

Identity Verification

- Ø1:n biometric search
- ØConfirm employment
- ØID Validation through standard government wide services
  - ØGovernment DB's
  - ØThreat risk

6

4

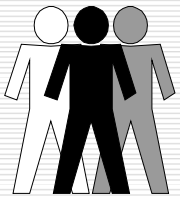
Enrollment

7

Card Production & Personalization

8

Issuer - Card Activation



PIV Activated for Operational Use

Numbers Indicate Functional Areas of Responsibility

Green functions manage Chain of Trust for Identity Verification

Implementation Solutions

- Multiple Implementation Methods are available
  - The challenge of compliance with PIV-I processes can be addressed by implementing a technology-based solution that automatically addresses all the PIV processes.
  - PACS Manufacturers that offer a solution that will deliver a single UI for PIV I enrollment are preferred.
  - PACS Manufacturers that have successful partnerships with PIV-I component providers are preferred.
    - Additionally, the VAR, (Systems Integrator) partner of the PACS Manufacturer is key to successful PIV II (Physical Security) deployment.
  - PACS Manufacturers with existing PIV-I experience preferred

(cont)

Implementation Solutions

- 1. Custom Middleware Combining Logical and PACS from Specialty Integrator.

  (Example: ST&D Article on Javits Federal Building)

  - PACS Manufacturer partners with Middleware Integrator and provides specific components of PIV-I
  - Directory based, open-standards compliant, for easy integration into legacy HR, IT Security and Physical Security systems
  - Supports workflow functionality to automate all steps of the PIV-I process and mandated separation of roles.
  - Forms the backbone of a system from which PIV-II can be built.
  - Multiple manufacturer UI interaction required for complete PIV-I Enrollment

Implementation Solutions

- 2. PACS Manufacturer Teams with Logical Solution Providers and Provides Specific Components of PIV-I. (Current Solution from most advanced PACS suppliers)
  - Logical Solution Partner Companies Include but are not limited to:
    - Viisage – Document capture and authentication component.
    - Crossmatch – Provides ten fingerprint capture hardware and software
    - ActivCard – Software to manage and personalize contact chip of smart card
  - Supports workflow functionality to automate all steps of the PIV-I process and mandated separation of roles.
  - Forms the backbone of a system from which PIV-II can be built.
  - Multiple manufacturer UI interaction required for complete PIV-I Enrollment

Implementation Solutions

- 3. PACS Manufacturer Teams with Logical Solution Provider and Provides Specific Components and UI of PIV-I. (Preferred Ultimate Solution)
  - PACS Manufacturer provides single UI to manage all aspects of PIV-I enrollment including Partner Company Application Management
    - This capability is requirement for PIV-II compliance
  - Logical Partner Companies Include but are not limited to:
    - Viisage – Document capture and authentication component.
    - Crossmatch – Provides ten fingerprint capture hardware and software
    - ActivCard – Software to manage and personalize contact chip of smart card
  - Supports workflow functionality to automate all steps of the PIV-I process and mandated separation of roles.
  - Forms the backbone of a system from which PIV-II can be built.

PIV ID Badge Components

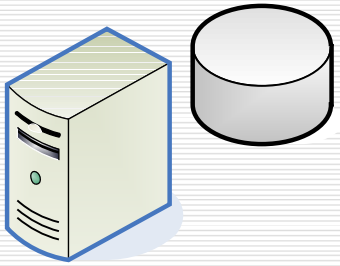
- Contactless Smart Chip Card
  - Information that is required
  - Expiration Date
  - Content that is not accessible via contactless
    - Biometric
    - Certificate

- Contact Smart Chip Card
  - Information that is required
  - Biometric containers
  - Requirements for High Security model

WORKFLOW FOR PIV-1

- Sponsorship
- ID Proofing and Registration
- Adjudication
- Issuance

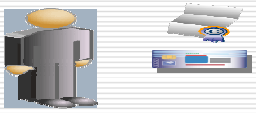
PIV-I Workflow: Application

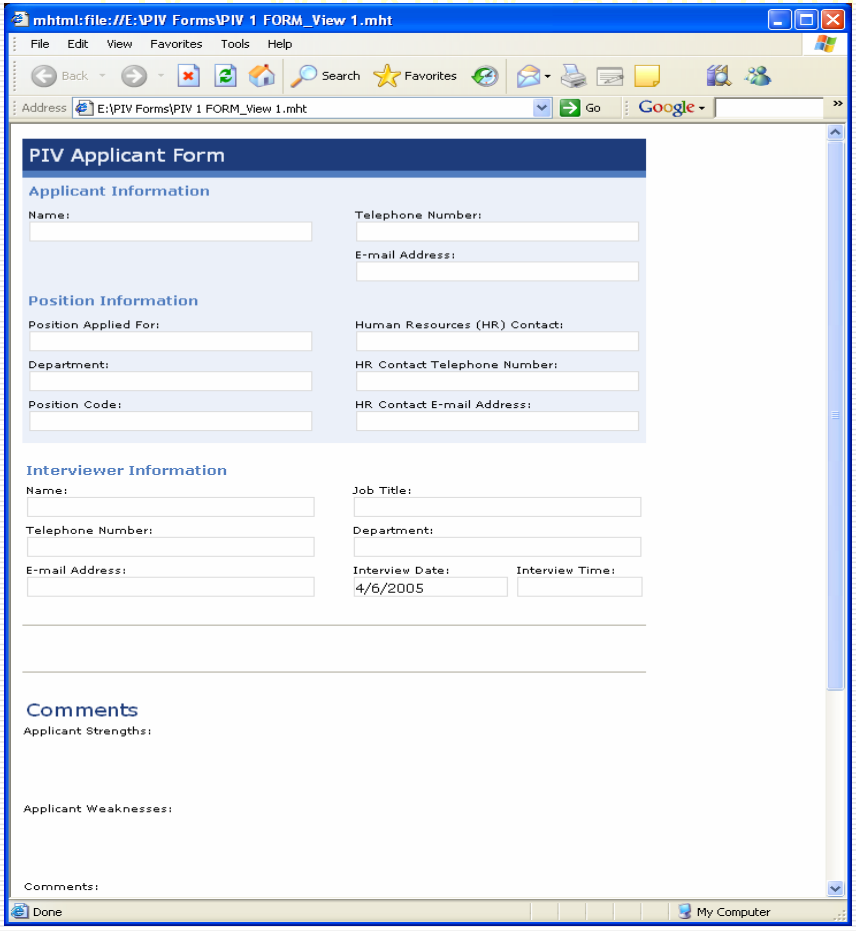


Identity Management System
IDMS

Applicant must apply for PIV credential and fill out a form

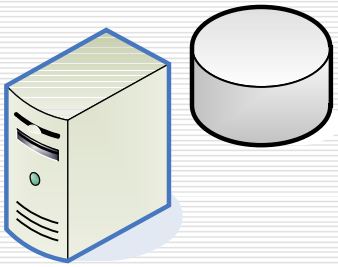
Applicant





Sponsorship → **ID Proofing and Registration** → **Adjudication** → **Issuance**

PIV-I Workflow: Sponsorship



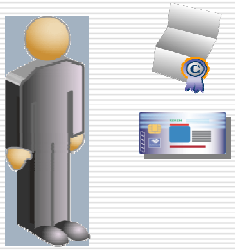
Identity Management System
IDMS

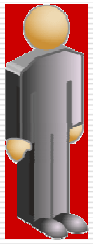
IDMS systems will send the applicant PIV form to employer / Sponsor

Employer / Sponsor will authorize the request for PIV credential.

Applicant

Employer/ Sponsor





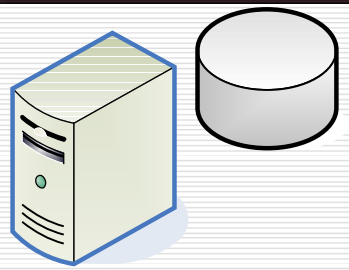
Sponsorship

ID Proofing and Registration

Adjudication

Issuance

ID Proofing and Registration



Identity Management System
IDMS

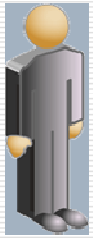
IDMS stores all PIV enrollment process records, including:

- I-9 breeder documents,
- 10 fingerprints
- Digital photograph

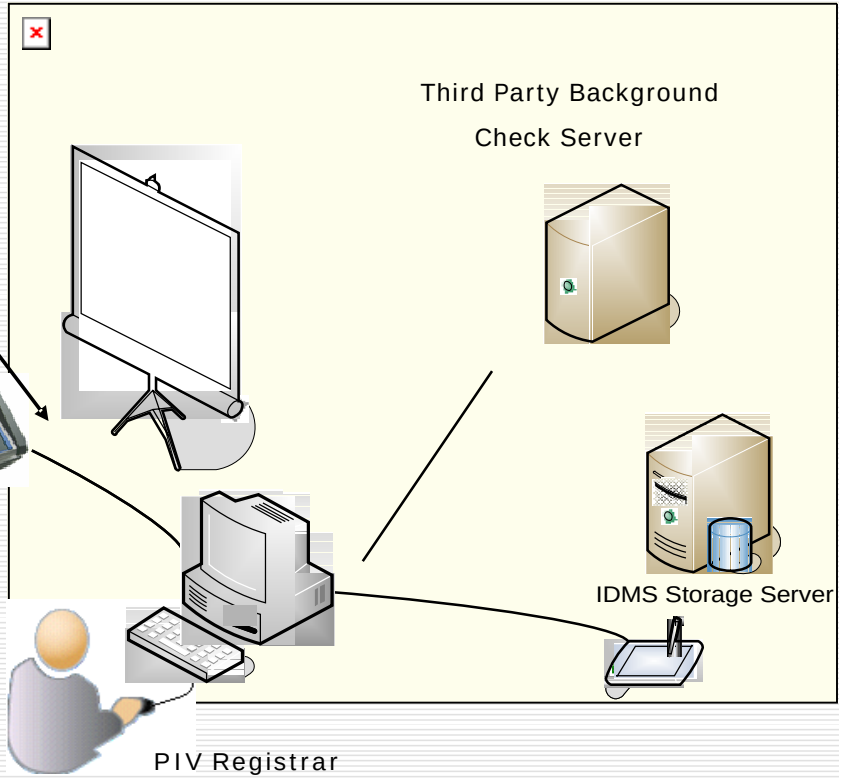
The PIV Registrar delivers a secured enrollment package to the IDMS for adjudication.

Enrollment
Registration / Binding

Applicant

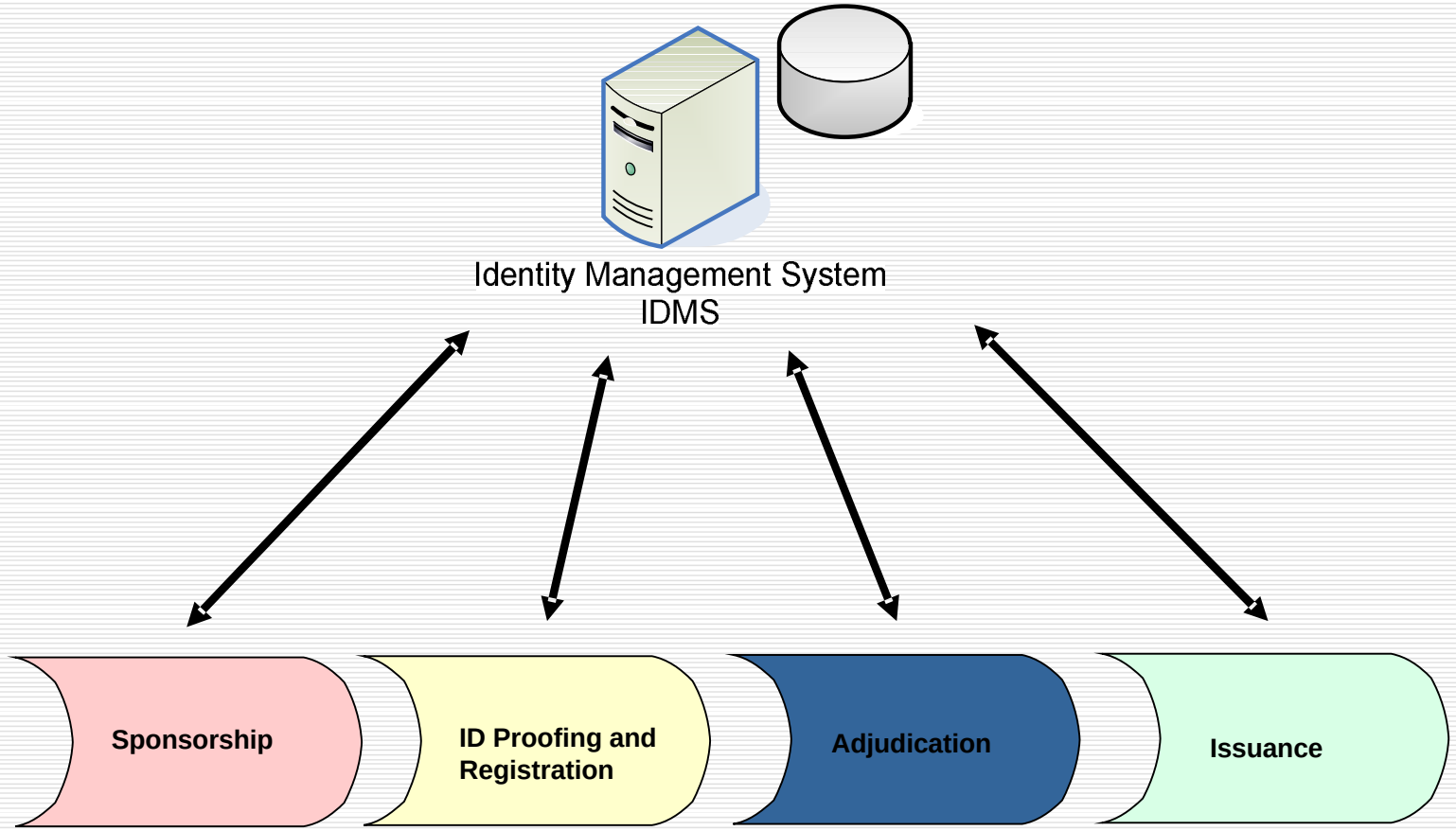


Applicant provide I-9 identity-source documents. Registrar scans and automatically verifies them.

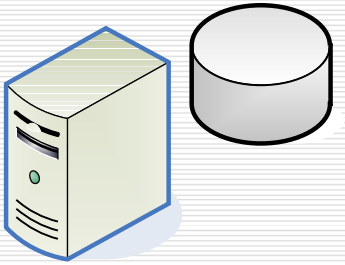


Sponsorship | **ID Proofing and Registration** | Adjudication | Issuance

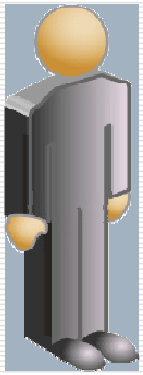
PIV-I Adjudication



PIV-I Card Issuance



Identity Management System
IDMS



Applicant is notified PIV Card is ready for pickup and activation

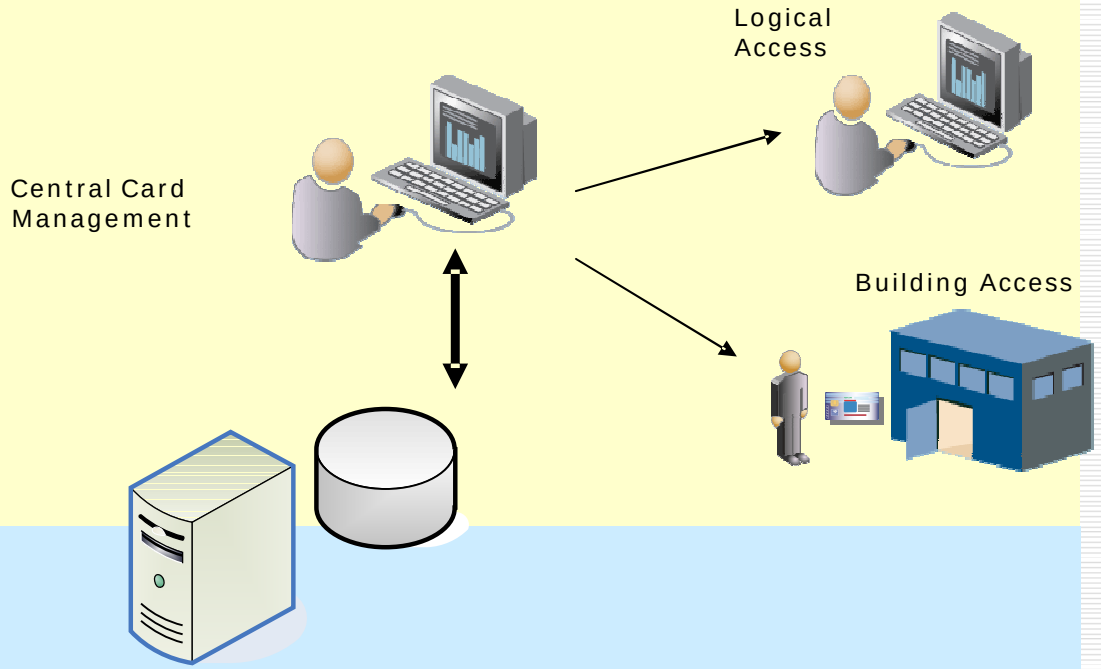
Issuer
Card Activation

Sponsorship → **ID Proofing and Registration** → **Adjudication** → **Issuance**

Migrating from PIV-I to PIV-II

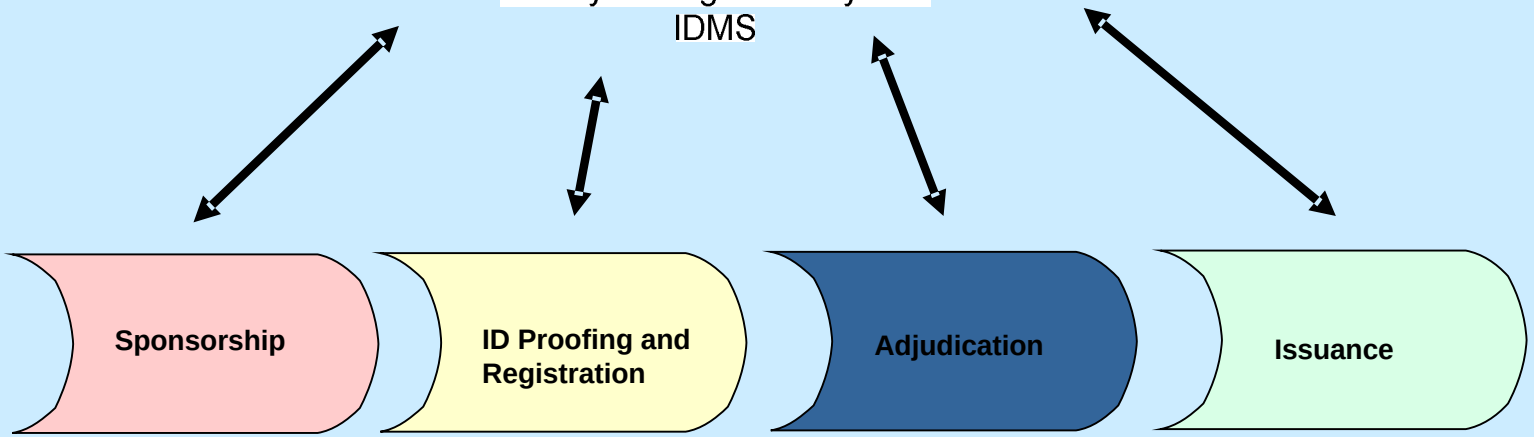
PIV-II

IDMS easily links to enterprise Card Management System to incorporate both Physical and Logical Access Control.



PIV-I

Identity Management System
IDMS



Key Issues to Convergence 1

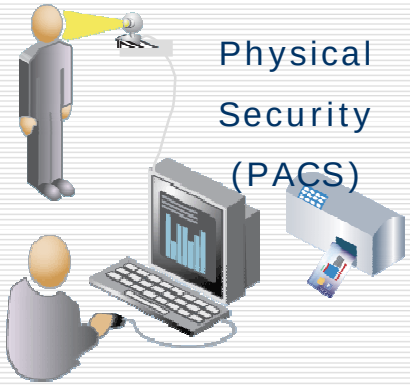
- Understanding Physical Access Infrastructure
  - Integration with Agency's Core IT Network
  - Agency-wide integration of Disparate PACSs
  - Replacement of Physical Access Readers
  - Upgrade of Physical Access Data Path

- Understanding of Logical Access Infrastructure
  - Enterprise Architecture for Desktop Authentication
  - Cryptographic Logon to Intranet and Web Applications
  - Integrated Solution for Email Signing and Encryption
  - Addition of Integrated Smart Card and Biometrics Reader or Replacement of Keyboard
  - Installation of Client Middleware

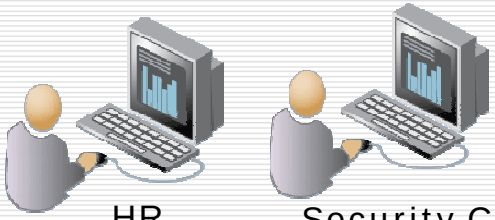
Key Issues to Convergence 2

- Integration of Physical and Logical Access Infrastructure
  - Integrated under one Network
  - Card/Credential Life Cycle Management
    - Suspension, Revocation and Termination
  - Common User Authentication Device
- Flexible Card Issuance System Components with Open Badging API
- Open Card Life Cycle Management API
- Interoperable Smart Card & Biometrics Solutions
- Reliable HR/Security Clearance Database and FIPS 201 Compliant Identity Vetting Process

PIV II Integrated Solution 1

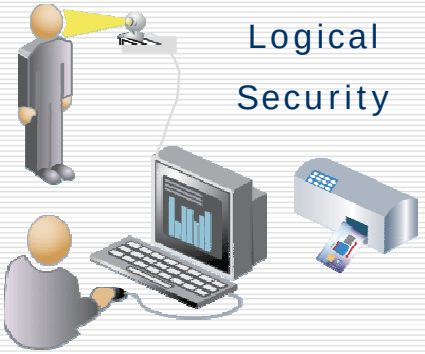


Physical Security (PACS)



HR

Security Clearance



Logical Security

FIPS 201 Compliant: Employee/Contractor Enrollment & Identity Vetting/Proofing, HR/Sec Clearance DB, and Cardholder Provisioning System

Privilege Granting to physical Access Security Infrastructure

Issue Badge: Legacy Technology Compatibility

Capture Photo and Biometrics at Enrollment

Upon Personal ID & Bio Verification Capture PIN, Personalize Contact & Contactless Integrate Circuit Chips

Issue & Activate Smart Card

PACS Badging Client

PACS Security Server

PACS Interface

Cardholder Database and Authentication Directory

Card Life Cycle API

CMS

Badge API

Card Issuance Client

Physical Access Security Infrastructure

Notify changes in card state

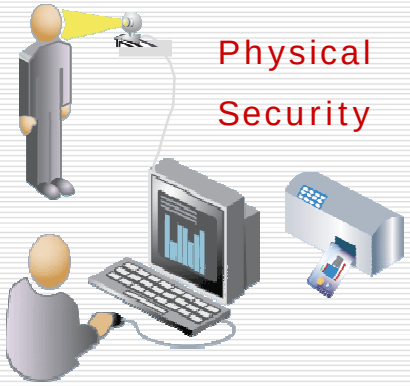
IT & Logical Access Security Infrastructure

- Contactless Operation
- FASC-N & PIN and/or Bio

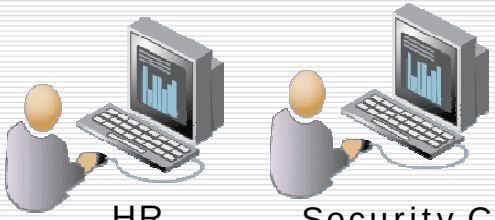
- Contact Operation with PIN and/or Bio
- Secure Windows Logon
- Email Sign & Encryption
- Secure Web & Application Access

Single UI PIV II Integrated Solution

(PACS Application and UI Managing All Processes)

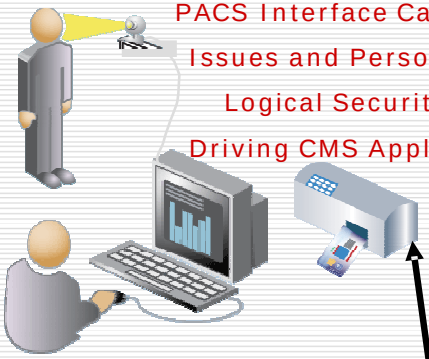


Physical Security



HR

Security Clearance



PACS Interface Captures, Issues and Personalizes Logical Security by Driving CMS Application

FIPS 201 Compliant: Employee/Contractor Enrollment & Identity Vetting/Proofing, HR/Sec Clearance DB, and Cardholder Provisioning System

Capture Photo and Biometrics at Enrollment

Upon Personal ID & Bio Verification
Capture PIN, Personalize Contact & Contactless Integrate Circuit Chips

Issue & Activate Smart Card

Privilege Granting to physical Access Security Infrastructure

Issue Badge: Legacy Technology Compatibility

PACS/IDMS Badging Client

PACS/IDMS Security Server

PACS/IDMS Interface

Cardholder Database and Authentication Directory

Card Life Cycle API

CMS

Badge API

Card Issuance Client

Physical Access Security Infrastructure

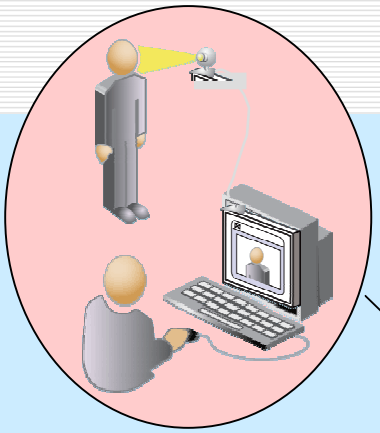
IT & Logical Access Security Infrastructure

Specialized PACS Application Functions as IDMS and Single UI for Integrated Management

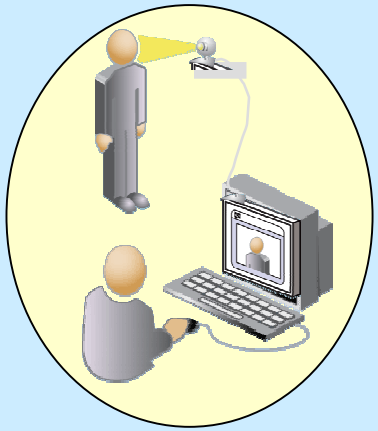
- Contactless Operation
- FASC-N & PIN and/or Bio

- Contact Operation with PIN and/or Bio
- Secure Windows Logon
- Email Sign & Encryption
- Secure Web & Application Access

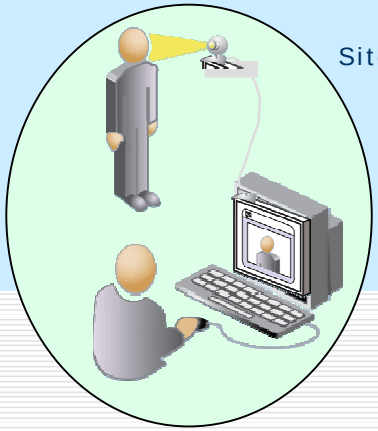
PIV-II: Distributed Registration with Central Management & Issuance



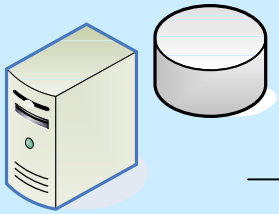
Site 1



Site 2

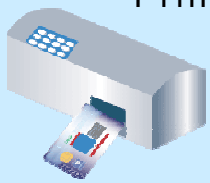


Site 3

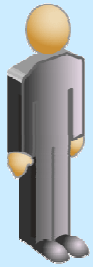


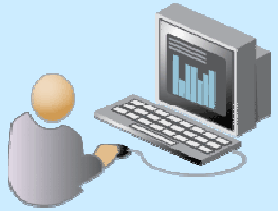
Identity Management System
IDMS

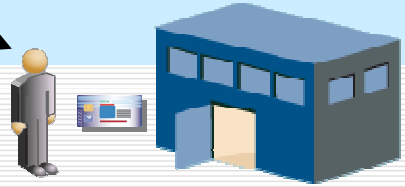
Central
Printing



Ship Card to
Issuance
Center







This architecture for PIV-II makes it easier to issue card in remote offices and cuts down on the need to procure card issuance systems.

End User Responsibility

- Although it is the intent of this standard, (FIPS 201), to specify mechanisms and support systems that provide high assurance personal identity verification, conformance to this standard does not assure that a particular implementation is secure. It is the implementer's responsibility to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner.

(extract from page VI of FIPS 201)

Information Resources

- Scott Rice Director of Government Sales
  - Lenel Systems International
  - srice1@lenel.com
- Jeremy Grant, VP
  - Maximus Enterprise Solutions
- Phillip Lee
  - Identity Alliance LLC

Lenel GSA Listed Value Added Reseller (VAR)

Wornall Secure Business Solutions

Peg Holen
Wornall Secure Business Solutions
Account Manager
8901 Washington
Kansas City, MO 64114
Peg.Holen@SecuritasSystems.com
[1] 816-333-6299
[1] 816-333-2796

GS-7F-5799P

Questions?

Thank You!